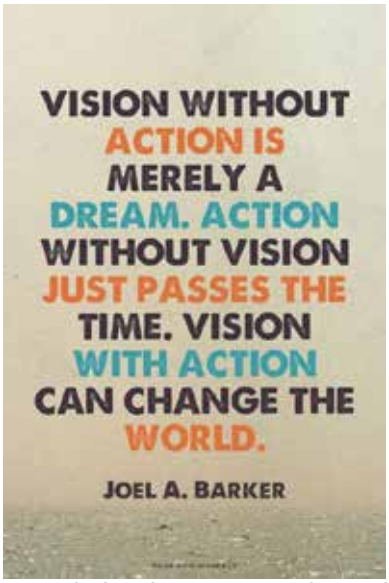
INDIA 2025-A DIGITAL DREAM

Dr. PRAKASH HEBALKAR



(Joel Barker was the first person to popularize the concept of paradigm shifts in the corporate world.)

- A Digital World (DW) will create a paperless dream for India with anytime-anywhere access for all its citizens.
- Services businesses enabled by underlying drivers of DW have already demonstrated key innovation – democratization of commerce-in-goods; crowd funding of start-ups; out-of-town and small mobile-based payment services etc.
- Realising the Digital Vision incorporates a whole new Digital Strategy, clear mapping of the deliverables and fail-safe implementation underscored by legal and regulatory support.

AN OVERVIEW:

The Digital World (DW) envisions a pivotal national shift from using information technology (IT) for point-solutions to creating an accessible, ubiquitous Digital World in India that enables personal and economic development for all citizens.

The driving force arises from the benefits from Moore's Law[1] on the cost of internet-enabled mobile devices with increased technical capabilities on the one hand, and the benefits flowing from Metcalfe's Law[2] from the network effect of growth of data communications capabilities (read internet) on the other hand. In short, **"the more the better"** – more people covered and participating, more economic activities covered, more governance activities covered etc.

Technologically, the expansion of the address-space of participants in the internet through the adoption of IPV6 has now enabled unattended devices to become participants, leading to the emergence of the Internet of Things (IOT). The internet now interconnects not just people to each other and not just physical world devices such as guided cars, power distribution networks, household appliances etc. to each other, but interconnects both people and devices.

[1]Moore's Law is a computing term which originated around 1970; the simplified version of this law states that processor speeds, or overall processing power for computers will double every two years, while simultaneously costs reduce by half.

[2]Metcalfe's law states the effect (value) of a telecommunications network is proportional to the square of the number of connected users of the system (n^2).

ANALYSIS & DISCUSSIONS:

The objective of creating a Digital World for India is to increase the velocity of economic activity.

1. The Digital World

The Digital World envisaged for India has some important characteristics:

A. **Virtual records** of value (assets), transactions, and identity that are entirely - paperless.

B. **Ubiquity of access** – Anytime, anywhere (location independent) access.

C. **Low thresholds for participation** –"inclusiveness focused".

A. Virtual Records

The essence of the Digital World (DW) is virtuality – representation of physical aspects of the "real" world in symbolic form for record-keeping, for transformations, for processing and for interaction with senses. Representation of documents by scanned images is the simplest example familiar to almost everyone touched by it to date. Extending that to contracts, evidence, land-assets, driving licenses, passports, visas etc. and indeed money itself, in an all-encompassing comprehensive manner is the objective of the DW.

Without virtualisation, the two other aspects outlined below would be impossible.

B Ubiquity of Access

The Digital World envisages that the limitations of time (e.g., working hours for banks) and place (e.g., physical ATM or bank branch) should no longer apply. Instead all transactions are allowed to occur electronically via one or more computing devices, mobile phones or IOT devices. This creates, when done successfully, an anytime-anywhere environment for all economic activity. Whether it is banking, border crossing, ecommerce, hospital admission or any activity requiring validation of identity and access, in the DW, the environment is set up to facilitate rather than block such activity.

C. Low Thresholds for Participation

The final characteristic of the Digital World is its use of low thresholds to enable mass participation. For example, a user simply needs to obtain an email address, use their registered mobile phone or similar method for unique identification in order to participate in the DW. Obtaining an email address requires only minimal information such as self-created handle (checked for availability and non-duplication) and a self-created password. The Central Government's JAN trio programme similarly requires minimal information and minimal (zero) money balance for account opening.

2. Benefits

A. Disintermediation

By virtualisation and direct interconnectivity among participants, intermediaries (with their cost and complications) become largely unnecessary. By connecting travellers and airlines, travel-agents become unnecessary for reservations and ticketing. By connecting buyers and suppliers, ecommerce and digital banking can make both stores and cash unnecessary.

B. Innovation

Services businesses have already demonstrated significant innovation enabled by the underlying drivers of the Digital World, including democratisation of the commerce-in-goods business.

- Peer-to-peer lending by individuals (in small amounts) to other individuals, adding up to adequately large amounts (e.g. Lendingclub).
- Crowd-funding of startup businesses (e.g. Kickstarter) by individuals in similar small bites.

- Out-of-town payment services (e.g. MPesa) and small payments by mobile phone based applications (e.g. Paypal and PayTM)
- And many more….

C. Governance Simplification

The disintermediation advantage described earlier can be a powerful tool for governance. The hitherto common middleman who facilitated obtaining permits, payments etc. can be eliminated by direct connectivity of citizens and government computers for citizen services such as for marriage certificates, death certificates, tax registration, tax payments etc.

3. Risks and Challenges

The Digital World is not inherently risky; rather the risks arise from the business model chosen to implement connectivity and access. For example, the physical risk to passengers using on-demand transportation services such as Uber, Ola or Meru arises from the large number of private car owners becoming drivers in the scheme and some drivers only participating on a sporadic basis, such as during surge pricing times. Surge pricing is designed as much to benefit from supply-demand mismatches financially as to increase supply of service providers in response to the incentives presented by the mismatch. Naturally, relatively little is known about these Johnny-come-lately drivers' behaviour or character, notwithstanding a crowd-sourced rating system.

In the case of payment systems, risks arise from the virtual nature of money transfers and the reliability of operators. "A prominent mobile operator who might own a payments bank could easily create accounts in the latter to which money transfers are redirected from mobile-linked bank accounts without the owner's knowledge or permission". Moreover, with identities unverified, traceability, in the event of default or in a series of related transactions of forensic interest is a problem. Absence of physical records may hinder recovery or prosecution if the judicial system is not a participant in the DW.

In the case of e-commerce, the convenience of cash on delivery (COD) payments engenders the risk of non-acceptance of delivery - a risk for merchants; in contrast, prepayment engenders the risk of delivery of bricks instead of mobile phones – a risk for the consumer. Both instances cited are real and have occurred in recent history.

All the above risks and all others get magnified manifold by the comprehensiveness of participation of all persons as economic actors. Any-to-any interactions are possible and indeed even encouraged (certainly by the creators of every App). The usual protections and risk-mitigation mechanisms such as credit ratings or credit checks before authorisation for participation (e.g. credit card issuance, insurance policy underwriting etc.) are either absent or harder to implement in a credible manner. Ubiquity creates an anytime-anywhere universe of transactions that provides little of the physical protections of a cashier's bullet-proof enclosure, or locked bank safe/vaults.

The Internet of Things (IOT) creates other risks, outlined by Bruce Schneider[3] in his new book, "Click Here to Kill Everybody", in which he warns about the rapidly evolving "one big connected system of devices".

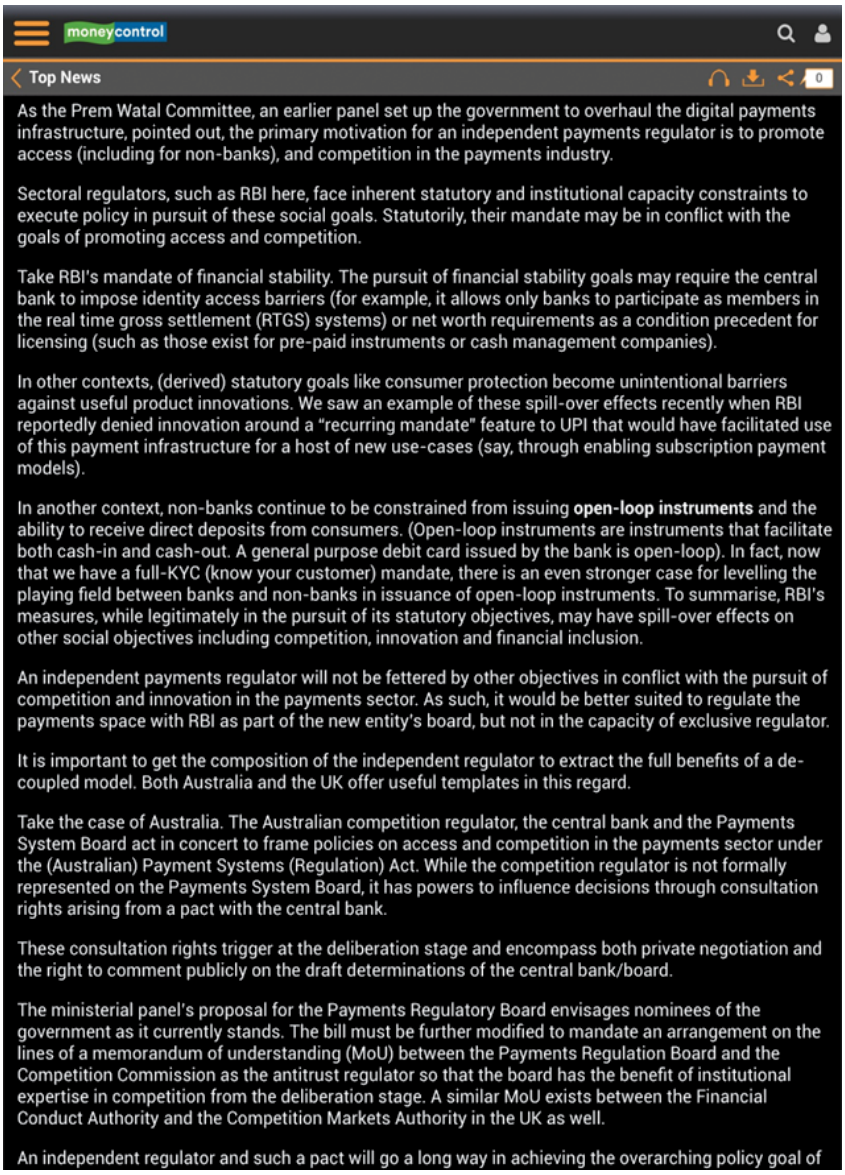
> One important difference between the Intenet we are used to and the Internet of the future is that computers can now directly affect the physical world. They help us drive our cars. They are embedded in our bodies in the form of heart monitors and defibrillators. They turn our heating and air conditioning on. They fly drones and control power plants. *Today we can be physically harmed by computers in ways that just were not possible before.* And that threat will increase as even more computers get physical capabilities. B.S. Schneider

[3]Mr Schneider, is a fellow at the Berkman Klein Center for Internet & Society at Harvard University; a Lecturer in Public Policy at the Harvard Kennedy School; a board member of the Electronic Frontier Foundation, AccessNow, and the Tor Project; an Advisory Board Member of the Electronic Privacy Information Center and VerifiedVoting.org; and a special advisor to IBM Security and the Chief Technology Officer at IBM Resilient.

One major societal risk is the conflict between regulation and innovation. It always exists in a pervasive or widespread and ubiquitous service. This is true of transportation and payment systems already, as explained below.

In the case of transportation, the on-demand model of Uber and its ilk ran into conflicts with the regulated taxi industry in many global cities, notably New York, London and Paris. In many cases, this was settled by limits on the number of vehicles. In others, it was resolved by regulations on driver qualifications or backgrounds. Consumer safety is an outstanding issue and will see competition between innovators and regulators to devise solutions.

In the case of payment systems, a similar conflict has presented itself between online wallets and debit cards. This too tends to get resolved, if at all, by quantitative restrictions or regulatory interventions of some kind such as 2-factor authentication that includes one-time-passwords or full blown-KYC (Know Your Customer) requirements. In the US, small value payments require no authentication (e.g. fuel purchase at a gas station) so the regulatory concern gets overlooked in the interests of velocity of business. The consumer liability limit of $50 under statutory protection plays a large role in calming consumer fears of misuse in this choice of regulation. Sometimes the conflict gets "resolved" by regulatory capture! In the case of payment systems, there is even competition between bureaucrats! Given alongside is some flavour of that:



moneycontrol

Top News

As the Prem Watal Committee, an earlier panel set up the government to overhaul the digital payments infrastructure, pointed out, the primary motivation for an independent payments regulator is to promote access (including for non-banks), and competition in the payments industry.

Sectoral regulators, such as RBI here, face inherent statutory and institutional capacity constraints to execute policy in pursuit of these social goals. Statutorily, their mandate may be in conflict with the goals of promoting access and competition.

Take RBI's mandate of financial stability. The pursuit of financial stability goals may require the central bank to impose identity access barriers (for example, it allows only banks to participate as members in the real time gross settlement (RTGS) systems) or net worth requirements as a condition precedent for licensing (such as those exist for pre-paid instruments or cash management companies).

In other contexts, (derived) statutory goals like consumer protection become unintentional barriers against useful product innovations. We saw an example of these spill-over effects recently when RBI reportedly denied innovation around a "recurring mandate" feature to UPI that would have facilitated use of this payment infrastructure for a host of new use-cases (say, through enabling subscription payment models).

In another context, non-banks continue to be constrained from issuing **open-loop instruments** and the ability to receive direct deposits from consumers. (Open-loop instruments are instruments that facilitate both cash-in and cash-out. A general purpose debit card issued by the bank is open-loop). In fact, now that we have a full-KYC (know your customer) mandate, there is an even stronger case for levelling the playing field between banks and non-banks in issuance of open-loop instruments. To summarise, RBI's measures, while legitimately in the pursuit of its statutory objectives, may have spill-over effects on other social objectives including competition, innovation and financial inclusion.

An independent payments regulator will not be fettered by other objectives in conflict with the pursuit of competition and innovation in the payments sector. As such, it would be better suited to regulate the payments space with RBI as part of the new entity's board, but not in the capacity of exclusive regulator.

It is important to get the composition of the independent regulator to extract the full benefits of a de-coupled model. Both Australia and the UK offer useful templates in this regard.

Take the case of Australia. The Australian competition regulator, the central bank and the Payments System Board act in concert to frame policies on access and competition in the payments sector under the (Australian) Payment Systems (Regulation) Act. While the competition regulator is not formally represented on the Payments System Board, it has powers to influence decisions through consultation rights arising from a pact with the central bank.

These consultation rights trigger at the deliberation stage and encompass both private negotiation and the right to comment publicly on the draft determinations of the central bank/board.

The ministerial panel's proposal for the Payments Regulatory Board envisages nominees of the government as it currently stands. The bill must be further modified to mandate an arrangement on the lines of a memorandum of understanding (MoU) between the Payments Regulation Board and the Competition Commission as the antitrust regulator so that the board has the benefit of institutional expertise in competition from the deliberation stage. A similar MoU exists between the Financial Conduct Authority and the Competition Markets Authority in the UK as well.

An independent regulator and such a pact will go a long way in achieving the overarching policy goal of

One hopes such competition to regulate results in the greater good.

4. Transition: Translating the Dream Into a Reality

> **Vision without execution is a hallucination** - Thomas Edison
> **Vision with action can change the world** - Joel A. Barker

This is best illustrated in India by the "garibi hatao" dream of the political powers in Delhi which remained a hallucination for five decades – a similar dream by the Chinese was turned into a transformed world in two decades.

Action towards transforming the dream into a Digital World involves:

A. Convergence and Omnichannel Architectures

Transition to a Digital World will require business organisations whether they deal in goods or services to develop "omnichannel" architectures. This is the unity and integrity of deliverables regardless of mode of access and delivery. In the case of commerce, for example, the same end result should be available whether at a physical store or on the internet; and whether directly or by referral (clickthrough) or a mix thereof. In the case of banking, a transaction should be possible to be carried out at a branch, via internet banking, or by physical or virtual cards at ATMs and retail point-of-sale devices.

B. Robust Infrastructure to Parallel the Physical One- "Too Big to Fail" is a Reality

Ubiquity is still far from achieved currently. Only an estimated 200 million Indians have some form of broadband access. Around 80% of mobile phones are feature phones with no smarts. Bureaucracies are uncomfortable without paper records. The list of areas of shortfall in the ubiquity objectives is long.

This calls for strong implementation mechanisms and a sense of urgency. It also requires robustness to ensure dependability of the data infrastructure that, at the very least, matches the dependability of the physical infrastructure which the masses can see and experience, and possibly even exceeds that so that its benefits are available even where the physical infrastructure is not (e.g. telemedicine advice in remote villages). As an exemplar, Tibetan-Chinese internet communications access is available right on top of Mount Everest[4]!

At the very least[5], availability of 4G service nationwide along with easy availability of gigabit fibre connectivity in urban areas are clear targets for 2025. The rapid build-out of 5G connectivity nationwide as global operational experience and standards develop are the stretch goals for 2025.

Establishing identity in a ubiquitous "all persons participating" environment is a major problem. Aadhar, according to the UIDAI, only confirms that in their database there exists an association between a (full set of) biometrics and an Aadhar number; any of the demographic details such as name, address, age, sex etc. are merely as provided by secondary evidence such as PAN cards or voter cards at the time of registration and so only as reliable as that secondary evidence. This implies that any fraud or mischief in the latter reflects in the UIDAI database too. The principal weak link in all such evidence is the collection of agents doing the registration and any corruption, malice or incompetence is mimicked in all such data.

Accordingly, establishing the credibility of a truly Universal ID system is a high priority task for the transition. The same problem arises for juridicial persons as the recent splash of news stories on fake loans and defunct companies illustrates. More on this later.

---

[4] EVEREST 2018 -REPORT FROM THE SUMMIT POSTED ON MAY 22, 2018

Hello everyone, reported that the entire team is standing on the summit of Everest As Ben mentioned it was a great summit day, not too many peoples, sunny and no wind. Team starting to summit from 6:27 till 7:28 they are going to take photos and start to descend to South Col soon.

[5] Broadband in the USA is defined as: The FCC retains the existing speed benchmark of 25 Mbps download/3 Mbps upload (25 Mbps/3 Mbps) for fixed services and examines the deployment of mobile services with minimum advertised speeds of 5 Mbps/1 Mbps, and those with a median speed of 10 Mbps/3 Mbps or higher. Feb 2, 2018.

C. Trust, Dependability, Crash Resistance – SLAs

These are implicit in an all-encompassing always-on economic environment. A digital payments system that fails rapidly destroys faith in digital payments. Similarly for other facilities, always-on is presumed and not a bonus. This demands very high levels of Service Level Agreements (SLAs) with vendors and subcontractors providing such connectivity – service levels relating to both geographical and temporal coverage, as well as responsiveness are crucial.

D. Regulation without Stifling Innovation

Regulation rapidly runs into a debate on two models of regulation: Regulation by Principles and Regulation by Prescription(s) or Directives. The former facilitates innovation, the latter is easier to implement. In India, the latter is more common. Since execution is 80% of strategy, a blend has to evolve. As an example, consider Competition regulation.

In Competition regulation, there is the issue of predatory pricing. The usual presumption is that incumbents build walls around themselves which are hard for insurgents to climb over or breakdown[6].

Predatory pricing then is an anti-competitive ploy that the successful incumbent can use to keep insurgents from maintaining their siege before they run out of men and material. In the real world this may have worked well. In a digital world, the insurgent now has deep pockets or a rich uncle (Uber, Flipkart, Tesla) and if he cannot win by strength of technology, he can use predatory pricing to win away customer volumes that are so key to his business model which depends critically on the network effect. Only principles based regulation can recognise this and adapt to this situation and then counteract such predatory pricing.

Directions for evolution of regulation of Fintech, Regtech, Insurtech etc. are still being explored as this report indicates:

> Traditional banking-sector participants are witnessing an emergence of marketplace lenders (MPLs) that is profoundly changing the way individuals and businesses within the financial community interact. An estimated $4.7 trillion in financial services revenue is at risk of being displaced by FinTech. This has made regulators increasingly aware that appropriate reform is needed, given MPLs' positioning in the financial services market, as well as their evolving business models and increasing institutional support.
>
> Policy-makers are attempting to develop a regulatory framework for MPLs that encourages growth and innovation, while balancing the need for addressing systemic risk and safeguarding consumers. The applicability of current regulations, and the language of those forthcoming, need to be clear and transparent so FinTech firms can appropriately navigate their industry's ever- changing environment. Failure to do so will have a dramatic impact on MPLs' potential to improve the world economy as a whole. Furthermore, the regulatory architecture must remain dynamic to handle the innovation coming from MPLs and the fast pace at which they move and evolve.
>
> This publication highlights the major differences in the current regulatory frameworks between China, the UK and the US with respect to MPLs. In particular, it focuses on the differences regarding investor protection and securities laws; clearing, settlement and segregation of client money; risk retention and capital requirements; secondary servicer requirements; tax incentives; promotion of SME lending; credit analysis and underwriting; data protection; regulatory reporting; registration and licensing; debt collection; and interest rate regulation. It then examines and assesses the concerns

[6]*Berkshire Hathway chairman Warren Buffet says his principle is: "The most important thing [is] trying to find a business with a wide and long-lasting moat around it... protecting a terrific economic castle with an honest lord in charge of the castle," he said. Warren Buffett believes* ***the "most important' factor to pick a successful investment is judging the durability of a company's competitive advantage or so-called "moat."*** *– Source CNBC*

that these differences raise for MPLs. We hope policy-makers will work together to create a standardized and accommodative framework for FinTech's growth and innovation. (World Economic Forum Report "The Complex Regulatory Landscape for FinTech").

E. Legal Support

The combinatorial explosion of interactions demands a matching response in error-proofing, error-mitigating (hence loss-mitigating and liability-mitigating) instruments. The problem is aggravated in the transition by the distinct nature of the physical interaction and the digital one. In a sense this can be seen already today in the ATM interaction - an interaction between the physical world of cash and the digital world of virtual banks. How is an identity fraud detected and rectified? Who bears liability? Is the standard Indian bank excuse when the captured image is not of the account holder that "the owner could have shared the password with an agent or office worker to get the cash on his behalf" challengeable? Today's incidence rate of such fraud will grow combinatorially with comprehensiveness of coverage such as by the Jan Dhan programme and the JAM trinity of measures.

This urgently calls for legislative and regulatory measures apportioning or capping/limiting liabilities of the actors[7] and providing for coverage of the risk by suitable insurance-like instruments.

15 U.S. Code § 1643 - Liability of holder of credit card

US Code

Notes

Authorities (CFR)

prev | next

(a) Limits on liability

(1) A cardholder shall be liable for the unauthorized use of a credit card only if—

(A) the card is an accepted credit card;

(B) the liability is not in excess of $50;

(C) the card issuer gives adequate notice to the cardholder of the potential liability;

(D) the card issuer has provided the cardholder with a description of a means by which the card issuer may be notified of loss or theft of the card, which description may be provided on the face or reverse side of the statement required by section 1637(b) of this title or on a separate notice accompanying such statement;

(E) the unauthorized use occurs before the card issuer has been notified that an unauthorized use of the credit card has occurred or may occur as the result of loss, theft, or otherwise; and

(F) the card issuer has provided a method whereby the user of such card can be identified as the person authorized to use it.

(2) For purposes of this section, a card issuer has been notified when such steps as may be reasonably required in the ordinary course of business to provide the card issuer with the pertinent information have been taken, whether or not any particular officer, employee, or agent of the card issuer does in fact receive such information.

(b) Burden of proof

In any action by a card issuer to enforce liability for the use of a credit card, the burden of proof is **upon the card issuer** to show that the use was authorized or, if the use was unauthorized, then the burden of proof is upon the card issuer to show that the conditions of liability for the unauthorized use of a credit card, as set forth in subsection (a), have been met.

(c) Liability imposed by other laws or by agreement with issuer Nothing in this section imposes liability upon a cardholder for the unauthorized use of a credit card in excess of his liability for such use under other applicable law or under any agreement with the card issuer.

(d) Exclusiveness of liability

Except as provided in this section, a cardholder incurs no liability from the unauthorized use of a credit card.

(Pub. L. 90–321, title I, §?133, as added Pub. L. 91–508, title V, §?502(a), Oct. 26, 1970, 84 Stat. 1126; amended Pub. L. 96–221, title VI, §?617, Mar. 31, 1980, 94 Stat. 182.),

An example of such a measure which applies to online use too is shown in the text box alongside. An extension of this measure, which gets into the Principles versus Prescriptions debate on regulations, may be requiring an additional factor authorisation before a large transaction can be considered authorised for payment by the ATM/Debit/credit card issuer.

i) Data Protection

Once universality of coverage is targeted and as it is achieved, trillions of data points are generated by the combinatorial power of billions of citizens with billions of goods and services as well as views and opinions. This "Data is the new Oil"[8] as Humby

[7]US Federal law limits consumers' liability for credit card fraud to $50 .... According to the Federal Fair Credit Billing Act: If your credit card - the physical card - is stolen and used by a crook, your issuer can hold you responsible for up to $50 in fraudulent charges. Oct 30, 2017.

said. Its value, both statistically (for insights) and qualitatively (e.g. for surveillance or marketing) is priceless. Accordingly its preservation and control of access become inevitable.

Laws and regulations regarding preservation and access are still evolving. The European General Data Protection Regulation (GPDR)[9] is one such effort. The Justice Sri Krishna committee report is triggering a similar effort in India.

Tension between the gatherers of data who wish to use and disseminate it for gain and the providers/generators of the data who wish to control access to their own data will continue. The judiciary, meanwhile, will keep applying the principle of"proportionality" in its attempt at fairness.

Metadata i.e., the mere existence of relationships (but not the details of the participants) and their structure, as well as anonymisation will be powerful tools for resolution of this tension. The medical fraternity already has major research efforts underway towards personalised medicine based on analysis of both metadata (e.g. gene variant correlation with phenotypes) and anonymisation (say of longitudinal data i.e., observations of the same individuals over long periods of time).

Jurisprudence, rather than legislation, is most likely to drive the evolution of legislation. The recent Aadhar judgment by the Supreme Court and its dissection with analysis by a legal commentator[10] is representative of this driving force.

ii) Evidence Act

As issues of liability will inevitably arise in such a massively combinatorial Digital World, the nature of evidence and standards of evidence too will have to evolve. Authenticity standards will have to evolve. Irrefutability principles will have to evolve. Standards for classification, e. g. for class action suits, will have to evolve and so on.

The willingness of the judiciary to cast a wide net for learning globally, to disseminate it within the community[11] and the development of legal education to remain up-to-date will be critical.

iii) Identity Protection and Theft

Identity establishment and verification are critical and yet remain a challenge even for technology: whether by biometrics (thumbprints) and image recognition (Apple Face ID), voice recognition (Amazon Alexa), puzzles, or artificial intelligence. False positives and false negatives both affect credibility of the mechanism in operation. Identity theft, proxies and stored data (e.g. fingerprints) bring up misidentification error probability. New solutions engender new challenges.

This is an evolutionary field and acceptance of "the cost of doing business" by service providers both of the technology costs and the liabilities of mistakes will be critical. A UIDAI type of stand that "we are never wrong" would be counterproductive.

---

[8]Clive Humby, UK Mathemetician and architect of Tesco's Clubcard, 2006 (widely credited as the first to coin the phrase): "Data is the new oil. It's valuable, but if unrefined it cannot really be used.

[9]The General Data Protection Regulation (EU) 2016/679 ("GDPR") is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.[1]

[10]The Aadhaar Judgment and the Constitution - I: Doctrinal Inconsistencies and a Constitutionalism of Convenience - Indian Constitutional Law and Philosophy by Gautam Bhatia@gautambhati88.

[11]Such as through the Maharashtra Judicial Academy.

18 U.S. Code § 1028 - Fraud and related activity in connection with identification documents, authentication features, and information

US Code

Notes

prev | next

(a) Whoever, in a circumstance described in subsection (c) of this section–

(1) knowingly and without lawful authority produces an identification document, authentication feature, or a false identification document;

(2) knowingly transfers an identification document, authentication feature, or a false identification document knowing that such document or feature was stolen or produced without lawful authority;

(3) knowingly possesses with intent to use unlawfully or transfer unlawfully five or more identification documents (other than those issued lawfully for the use of the possessor), authentication features, or false identification documents;

(4) knowingly possesses an identification document (other than one issued lawfully for the use of the possessor), authentication feature, or a false identification document, with the intent such document or feature be used to defraud the United States;

(5) knowingly produces, transfers, or possesses a document-making implement or authentication feature with the intent such document-making implement or authentication feature will be used in the production of a false identification document or another document-making implement or authentication feature which will be so used;

(6) knowingly possesses an identification document or authentication feature that is or appears to be an identification document or authentication feature of the United States or a sponsoring entity of an event designated as a special event of national significance which is stolen or produced without lawful authority knowing that such document or feature was stolen or produced without such authority;

(7) knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law; or

(8) knowingly traffics in false or actual authentication features for use in false identification documents, document-making implements, or means of identification; shall be punished as provided in subsection (b) of this section.

Source: Wikipedia

F. Business Strategy

Apart from multi-channel architectures, business organisations will have to develop a whole Digital Strategy involving all facets of business, such as sales, marketing, supply chains, post warranty support, customer complaint handling, financing etc. and their impact on profitability as well as growth. Digital Strategy for business is a topic that requires its own focus and is best left for another day and time.

It is nevertheless critical.

CONCLUSIONS:

The realisation of the Digital Vision requires a clear enunciation of the deliverables and good implementation. The devil is always in the details.

A dependable and adequate digital infrastructure that truly covers the entire country is a critical requirement. A dependable identity mechanism that withstands technological and process failure is another. In this regard the record of Aadhar is un-established to date. A fail-safe transaction platform that supports genuine transactions to the benefit of all participants in a transaction and prevents dubious ones is a third.

Consumer protection mechanisms that are technologically up to date and backed by legislative and effective regulatory support, is another critical requirement. A legislative environment that is in keeping with the times is yet another.

A well managed transition from the current to this digital world will indeed be a grand paradigm shift for India that will accelerate the velocity of economic activity!